PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224189
(43)Date of publication of application : 17.08.1999

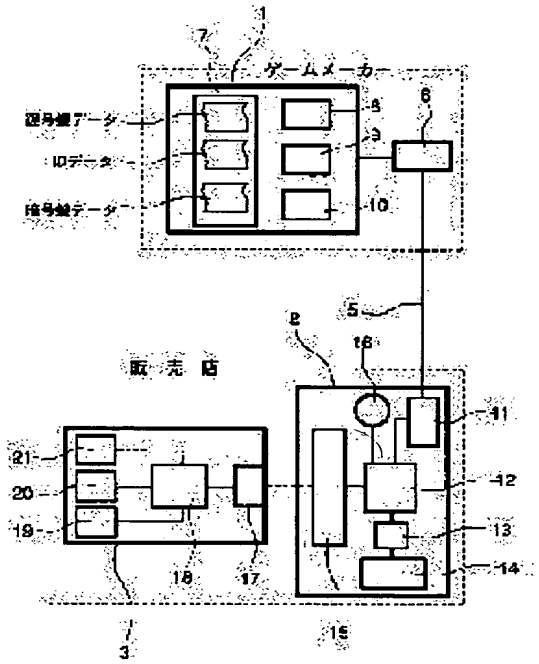
(51)Int.CI. G06F 9/06
G06F 12/14
G09C 1/00
H04L 9/32

(21)Application number : 10-041253
(22)Date of filing : 06.02.1998

(71)Applicant : NIPPON CHEMICON CORP
(72)Inventor : YAMAMOTO KAZUYUKI

(54) DECODING KEY DATA WRITING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a decoding key data writing system by which decoding key data are not appropriated by a third person even at the time of distribution or writing in an IC card.
SOLUTION: This system consists of a hot computer 1 provided with a storage device 7 for storing decoding key data for decoding ciphered program data, identifying data intrinsically imparted to the IC card and cipher key data corresponding to the identifying data and with a cipher generating device 8 for enciphering decoding key data, the IC card 3 provided with a memory part 19 for storing decoding key data, identifying data and cipher key data corresponding to identifying data, with a cipher processing part 21 for restoring enciphered decoding key data and with a control part 18, an IC card reader/ writer 2 and a communication means 5 connecting the host computer to the IC card reader/writer 2. Enciphered decoding key data are written in the IC card by cipher key data corresponding to identifying data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－224189

(43)公開日　平成11年(1999)８月17日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｃ
	12/14	３２０		12/14	３２０Ｂ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ａ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｃ

審査請求　未請求　請求項の数４　ＦＤ　（全９頁）

(21)出願番号　特願平10－41253

(22)出願日　平成10年(1998)２月６日

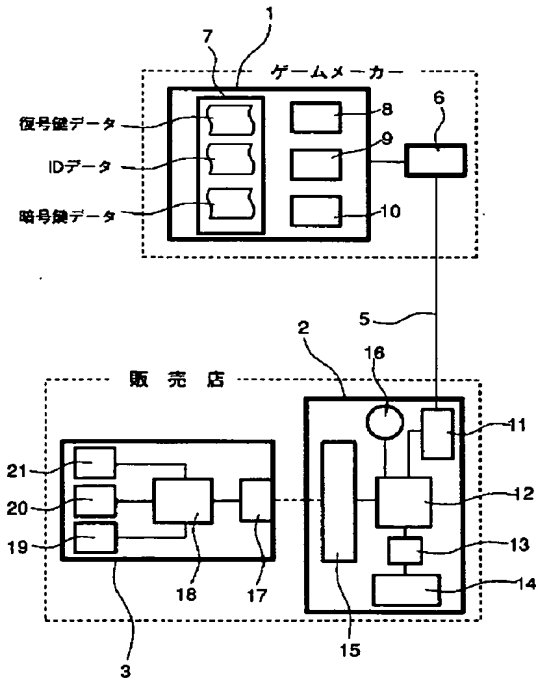
(71)出願人　000228578
日本ケミコン株式会社
東京都青梅市東青梅１丁目167番地の１
(72)発明者　山本　和行
東京都青梅市東青梅一丁目167番地の１
日本ケミコン株式会社内
(74)代理人　弁理士　日高　一樹　（外１名）

(54)【発明の名称】　復号鍵データの書き込みシステム

(57)【要約】

【課題】　配信時やＩＣカードへの書き込み時においても第三者によって、復号鍵データが盗用されることのない復号鍵データの書き込みシステムを提供する。

【解決手段】　暗号化されているプログラムデータを復号する復号鍵データとＩＣカードに固有に付与された識別データとこの識別データと対応付けられた暗号鍵データとを記憶する記憶装置７と、前記復号鍵データを暗号化する暗号生成装置８とを具備するホストコンピュータ１と、前記復号鍵データおよび前記識別データおよび識別データと対応付けられた暗号鍵データとを記憶するメモリ部１９と、前記暗号化された復号鍵データを復元する暗号処理部２１と、制御部１８とを具備するＩＣカード３と、ＩＣカードリーダライタ２と、前記ホストコンピュータ１とＩＣカードリーダライタ２とを接続する通信手段５と、から成り、前記識別データに対応付けられた暗号鍵データにより、暗号化された復号鍵データがＩＣカード３に書き込まれるようにする。



1

【特許請求の範囲】

【請求項１】　光記憶ディスク等の記憶媒体に暗号化されて記憶されているプログラムデータを復号する復号鍵データとＩＣカードに固有に付与されたＩＤ等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する記憶装置と、前記暗号鍵データにより所定のアルゴリズムに基づいて前記復号鍵データを暗号化する暗号生成装置とを具備するホストコンピュータと、

前記復号鍵データおよびＩＣカードに固有に付与されたＩＤ等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する不揮発性のメモリ部と、前記ホストコンピュータより出力される暗号化された復号鍵データを前記メモリ部に記憶されている暗号鍵データによって復元する暗号処理部と、これら各部を制御する制御部とを具備するＩＣカードと、

このＩＣカードに書き込み、読み出しを行うＩＣカードリーダライタと、

前記ホストコンピュータとＩＣカードリーダライタとを接続する通信手段と、から成り、

前記暗号化された復号鍵データがホストコンピュータよりＩＣカードに書き込まれる際に、前記ＩＤ等の識別データがＩＣカードより読み出され、そのＩＤ等の識別データに対応付けられてホストコンピュータの記憶装置に記憶されている暗号鍵データにより、暗号生成装置にて暗号化された復号鍵データが、通信手段およびＩＣカードリーダライタを介してＩＣカードに出力されることを特徴とする復号鍵データの書き込みシステム。

【請求項２】　前記復号鍵データが、ＩＣカードにおいて前記暗号化された状態の復号鍵データとして記憶されており、必要に応じて復号鍵データに復元されるようになっている請求項１に記載の復号鍵データの書き込みシステム。

【請求項３】　前記ＩＣカードのメモリ部に記憶された暗号鍵データが、ＩＣカードより読み出し不可とされている請求項１または２に記載の復号鍵データの書き込みシステム。

【請求項４】　所定長のランダムデータを生成するランダムデータ生成手段と、前記メモリ部に記憶されている暗号鍵データにより暗号化されたランダムデータを復元する復元手段と、この復元されたランダムデータと前記ランダムデータ生成手段により生成された所定長のランダムデータとを比較する比較手段とが前記ホストコンピュータに設けられるとともに、前記所定長のランダムデータを前記メモリ部に記憶された暗号鍵データにより暗号化する暗号生成部が前記ＩＣカードに設けられ、暗号化された復号鍵データがＩＣカードに出力される際に、前記所定長のランダムデータがホストコンピュータからＩＣカードに出力され、ＩＣカードにおいてこのランダムデータが、前記暗号生成部により暗号化され、この暗号化されたランダムデータがホストコンピュータに返送、前記復元手段により復元されるとともに、前記比較手段によって元のランダムデータと比較され、これらが一致した場合に暗号化された復号鍵データがホストコンピュータより出力されるようになっている請求項１～３のいずれかに記載の復号鍵データの書き込みシステム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術の分野】本発明は、ＣＤＲＯＭやＤＶＤ等の記憶媒体に暗号化されて記憶されているゲームソフト等のプログラムデータを復号する復号鍵データ（ライセンス鍵データ）の盗用を防止することのできる復号鍵データの書き込みシステムに関する。

【０００２】

【従来の技術】近年、ＣＤＲＯＭやＤＶＤ等の記憶媒体に記憶されたゲームソフト等のプログラムデータを不正にコピーして使用する不正使用が社会的な問題となっている。

【０００３】これら不正使用を防止するための方法として、これら光記憶媒体であるＣＤＲＯＭやＤＶＤ等に記憶されるプログラムデータを暗号鍵データ等により暗号化して記憶しておき、これら暗号化されたプログラムデータを復号する復号鍵データ（ライセンス鍵データ）を入手しないと、暗号化されたプログラムデータを平文データに復号することができないようにして、不正なコピーや使用を防止する方法が提案されている。

【０００４】しかしながら、これら復号鍵データ（ライセンス鍵データ）を用いた場合においては、暗号化されたプログラムデータそのものを複製しても、そのまま使用することができないようにすることはできるものの、この復号鍵データ（ライセンス鍵データ）が第三者によって盗用、入手されると、容易に不正な使用が可能となってしまうという問題点があるため、これら復号鍵データ（ライセンス鍵データ）を盗用されないように、ユーザーに配布する必要があった。

【０００５】これら盗用の問題を解決するために、近年ではこれら復号鍵データ（ライセンス鍵データ）をＩＣカード等の電子記憶媒体に記憶して、各ユーザーにライセンスカードとして配布し、ユーザーにおいても復号鍵データ（ライセンス鍵データ）が不明なようにして、そのＩＣカードがないとプログラムデータを使用できないようにする試みがなされている。

【０００６】

【発明が解決しようとする課題】しかしながら、これらＩＣカードを用いた復号鍵データ（ライセンス鍵データ）の配布方法は、復号鍵データ（ライセンス鍵データ）の盗用を一元的には防止できるものの、通常においてこれらライセンスカードは、各販売店等にて、前記ＩＣカードに復号鍵データ（ライセンス鍵データ）が書き込まれているため、これら各販売店等に復号鍵データ（ライセンス鍵データ）を配信しＩＣカードへ書き込む

際において、復号鍵データ（ライセンス鍵データ）が盗用される可能性が高いという問題があった。

【０００７】よって、本発明は上記した問題点に着目してなされたもので、各販売店等への配信時やＩＣカードへの書き込み時においても第三者によって、復号鍵データ（ライセンス鍵データ）が盗用されることのない復号鍵データの書き込みシステムを提供することを目的としている。

【０００８】

【課題を解決するための手段】前記した問題を解決するために、本発明の復号鍵データの書き込みシステムは、光記憶ディスク等の記憶媒体に暗号化されて記憶されているプログラムデータを復号する復号鍵データとＩＣカードに固有に付与されたＩＤ等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する記憶装置と、前記暗号鍵データにより所定のアルゴリズムに基づいて前記復号鍵データを暗号化する暗号生成装置とを具備するホストコンピュータと、前記復号鍵データおよびＩＣカードに固有に付与されたＩＤ等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する不揮発性のメモリ部と、前記ホストコンピュータより出力される暗号化された復号鍵データを前記メモリ部に記憶されている暗号鍵データによって復元する暗号処理部と、これら各部を制御する制御部とを具備するＩＣカードと、このＩＣカードに書き込み、読み出しを行うＩＣカードリーダライタと、前記ホストコンピュータとＩＣカードリーダライタとを接続する通信手段と、から成り、前記暗号化された復号鍵データがホストコンピュータよりＩＣカードに書き込まれる際に、前記ＩＤ等の識別データがＩＣカードより読み出され、そのＩＤ等の識別データに対応付けられてホストコンピュータの記憶装置に記憶されている暗号鍵データにより、暗号生成装置にて暗号化された復号鍵データが、通信手段およびＩＣカードリーダライタを介してＩＣカードに出力されることを特徴としている。この特徴によれば、ホストコンピュータより販売店およびＩＣカードに復号鍵データが配信、書き込まれる際に、ホストコンピュータより出力される復号鍵データが、ＩＣカードに個別に付与されたＩＤ等の識別データと関連付けられた暗号鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体が盗用されることなく、復号鍵データを販売店およびＩＣカードに配信、書き込むことができる。

【０００９】本発明の復号鍵データの書き込みシステムは、前記復号鍵データが、ＩＣカードにおいて前記暗号化された状態の復号鍵データとして記憶されており、必要に応じて復号鍵データに復元されるようになっていることが好ましい。このようにすれば、ＩＣカード内部において、復号鍵データが暗号化された状態にて記憶されているため、第三者によって復号鍵データ自体をＩＣカード内部より読み出されて盗用されることを防ぐことができる。

【００１０】本発明の復号鍵データの書き込みシステムは、前記ＩＣカードのメモリ部に記憶された暗号鍵データが、ＩＣカードより読み出し不可とされていることが好ましい。このようにすれば、仮にＩＣカードより暗号化された復号鍵データが盗用されたとしても、第三者によってＩＣカードより暗号鍵データが読み出されて、前記暗号化された復号鍵データが復元されることを防止できる。

【００１１】本発明の復号鍵データの書き込みシステムは、所定長のランダムデータを生成するランダムデータ生成手段と、前記メモリ部に記憶されている暗号鍵データにより暗号化されたランダムデータを復元する復元手段と、この復元されたランダムデータと前記ランダムデータ生成手段により生成された所定長のランダムデータとを比較する比較手段とが前記ホストコンピュータに設けられるとともに、前記所定長のランダムデータを前記メモリ部に記憶された暗号鍵データにより暗号化する暗号生成部が前記ＩＣカードに設けられ、暗号化された復号鍵データがＩＣカードに出力される際に、前記所定長のランダムデータがホストコンピュータからＩＣカードに出力され、ＩＣカードにおいてこのランダムデータが、前記暗号生成部により暗号化され、この暗号化されたランダムデータがホストコンピュータに返送、前記復元手段により復元されるとともに、前記比較手段によって元のランダムデータと比較され、これらが一致した場合に暗号化された復号鍵データがホストコンピュータより出力されるようになっていることが好ましい。このようにすれば、書き込みがなされるＩＣカードが正規のＩＣカードであるか否かを暗号化された復号鍵データを出力する以前にホストコンピュータが確認できるばかりか、ホストコンピュータに識別データと関連付けて記憶されている復号鍵データに誤りが無いか否かを確認することもできる。

【００１２】

【発明の実施の形態】以下、図面に基づいて本発明の実施形態を説明する。

【００１３】図１は、本実施例における復号鍵データの書き込みシステムを用いたライセンスカードシステムを示す図であり、図２は本実施例における復号鍵データの書き込みシステムの各構成を示すブロック図であり、図３は、本実施例におけるホストコンピュータに用いた暗号生成装置での処理内容を示す図であり、図４は、本実施例におけるＩＣカードに用いた暗号処理部での処理内容を示す図であり、図５は、本実施例において用いた暗号処理アルゴリズムの処理概要を示す図であり、図６は、ホストコンピュータとＩＣカード発行装置とＩＣカードとの処理動作を示す図である。

【００１４】本実施例では、本発明の復号鍵データの書き込みシステムをゲームプログラムのライセンスカード

システムに応用したものである。

【００１５】本実施例のゲームプログラムのライセンスカードシステムは、図１に示されるような構成とされており、ゲームメーカーに配置されたホストコンピュータ１と、各販売店に設置されたＩＣカード発行装置２と、ライセンス鍵である復号鍵データが書き込み、記憶されるＩＣカード３と、このＩＣカード３を装着可能とされたゲームプログラムの再生装置４と、暗号化されたゲームプログラムデータが記憶され、この再生装置４にて再生されるＣＤＲＯＭと、から主に構成されており、前記の暗号化されたゲームプログラムデータが記憶されたＣＤＲＯＭは、ゲームメーカーより各ユーザーに配付され、各販売店にてそのＣＤＲＯＭに対応する前記復号鍵データが、前記ＩＣカード３に書き込むことにより販売され、各ユーザーがそのＩＣカード３を再生装置４に装着することにより、ＩＣカード３に記憶されている復号鍵データが読み出されて、ＣＤＲＯＭに記憶されている暗号化されたゲームプログラムデータが復号されて実行可能なようになっている。

【００１６】前記ライセンスカードシステムに用いた本実施例の復号鍵データの書き込みシステムは、図２に示されるような構成とされており、前記ホストコンピュータ１は、その特徴として、ハードディスク等の記憶装置７内部に、ライセンス鍵である復号鍵データ（ＰＴ）と、データベース化された各ＩＣカード３に固有に付与されているＩＤデータおよび各ＩＤデータと１対１に対応付けられた暗号鍵データ（ＫＡ）とが記憶されており、さらにこの復号鍵データ（ＰＴ）を前記暗号鍵データ（ＫＡ）により暗号化するとともに、ＩＣカード３より返送されてくる暗号化されたランダムデータ（ＡＲ）を復元する暗号生成装置８と、所定長のランダムデータ（ＴＲ）を生成するランダムデータ生成装置９と、これらランダムデータ（ＴＲ）と前記ＩＣカード３より返送され暗号生成装置８によって復元された復元ランダムデータ（ＦＲ）とを比較する比較部１０が設けられており、このホストコンピュータ１は、通信モデム６および通信回線５を介して前記ＩＣカード発行装置２と接続されている。

【００１７】この各販売店に設置されたＩＣカード発行装置２は、図２に示されるような構成とされており、前記通信モデム６とのデータ通信を実施する通信モデム部１１と、ＩＣカード３が挿入されることによりＩＣカード３とのデータのやり取りを実施するＩＣカードリーダライタ部１５と、表示部としてのＬＣＤパネル１４と、このＬＣＤパネル１４の表示動作を制御するＬＣＤドライバ１３と、発行スイッチ１６と、これら各部の制御を実施するマイクロプロセッシングユニット（ＭＰＵ）１２が設けられ、このＭＰＵ１２の内部には内部ＲＯＭ（図示せず）が設けられ、ＭＰＵ１２が行う制御動作が記述されたプログラムが予め記憶、格納されている。

【００１８】また、前記ＩＣカード３の構成は、図２に示されるようになっており、本実施例では、各ＩＣカード３には固有のＩＤが付与されており、これらＩＤデータおよびこのＩＤデータと１対１に対応付けられた暗号鍵データ（ＫＢ）並びに前記ホストコンピュータ１より出力される暗号化された復号鍵データ（ＰＡ）とを記憶する不揮発性メモリであるＥＥＰＲＯＭ部１９と、各種演算等において使用されるメモリ部２０と、後述する所定のアルゴリズムに基づき、前記ＥＥＰＲＯＭ部１９に記憶されている暗号鍵データ（ＫＢ）により、ホストコンピュータ１より出力される所定長のランダムデータ（ＴＲ）の暗号化および前記暗号化された復号鍵データ（ＰＡ）の復元を実施する暗号処理部２１と、前記ＩＣカードリーダライタ部１５とのデータのやり取りを実施する通信部１７と、これら各部の制御等を実施する制御部１８とが設けられており、前記ＥＥＰＲＯＭ部１９にはＩＣカード３に付与された前記ＩＤデータおよび暗号鍵データ（ＫＢ）が予め記憶されており、この暗号鍵データ（ＫＢ）は、図５に示されるように、前記ホストコンピュータ１に記憶されている暗号鍵データ（ＫＡ）と所定の規則に基づいて双方の暗号鍵データで暗号化されたデータを復元可能な鍵データ組として１セットとされており、ＩＣカード３外部よりその出力が指示されても、暗号鍵データ（ＫＡ）が出力されないように、前記ＥＥＰＲＯＭ部１９の特定のアドレスに記憶されるようになっており、このアドレスの読み出し指示は、前記暗号処理部２１からの出力のみが有効となるように制御部１８にプログラムされている。

【００１９】本実施例において、前記ホストコンピュータ１内部に設けられた暗号生成装置８での暗号化処理の内容は、図３に示されるようになっており、書き込みがなされるＩＣカード３のＩＤに対応する暗号鍵データ（ＫＡ）が入力されることにより、この暗号鍵データ（ＫＡ）に基づき、入力された復号鍵データ（ＰＴ）をべき乗剰余演算アルゴリズムにより演算処理し、同一桁数の配列が異なる暗号化された復号鍵データ（ＰＡ）とするとともに、前記ＩＣカード３より送られてきた、暗号鍵データ（ＫＢ）に基づき暗号化された暗号化ランダムデータ（ＡＲ）を、上記の復号鍵データ（ＰＴ）の暗号化処理同様に、暗号鍵データ（ＫＡ）に基づき、べき乗剰余演算アルゴリズムにより演算処理することにより、復元ランダムデータ（ＦＲ）に復元されるようになっている。

【００２０】また、ＩＣカード３内部に設けられた前記暗号処理部２１の処理内容は、図４に示されるようになっており、予め前記ＥＥＰＲＯＭ部１９に記憶されている暗号鍵データ（ＫＢ）が入力されることにより、この暗号鍵データ（ＫＢ）に基づき、ホストコンピュータ１より出力される所定長のランダムデータ（ＴＲ）をべき乗剰余演算アルゴリズムにより演算処理し、同一桁数の

配列が異なる暗号化ランダムデータ（ＡＲ）とするとともに、前記ホストコンピュータ１にて暗号鍵データ（ＫＡ）により暗号化された復号鍵データ（ＰＡ）を、べき乗剰余演算アルゴリズムにより演算処理し、復号鍵データ（ＰＴ）に復元するようになっている。

【００２１】これら本実施例において用いた、前記べき乗剰余演算アルゴリズムの処理内容は、図５に示されるようになっており、暗号化処理においては、図５（ａ）に示すように、入力されたデータ列の各桁の数値を、所定の暗号鍵データ（ＫＡ）により乗数計算し、その計算値の所定の桁（本実施例では最小桁）の数値を出力データとして暗号化を実施するようになっており、これら暗号化されたデータ列の復元を実施する復元処理においては、図５（ｂ）に示すように、前記暗号化に用いた暗号鍵データと対をなす所定の暗号鍵データ（ＫＢ）により、暗号化と同様の処理を実施することにより、元のデータ列が復元されるようになっている。

【００２２】これらホストコンピュータ１とＩＣカード発行装置２とＩＣカード３との間におけるデータ等のやり取りおよびその処理内容は、図６に示されるようになっており、ＩＣカード３がＩＣカード発行装置２のＩＣカードリーダー８に挿入されると、ＩＣカード３の挿入が検出され、ＩＣカード３に対して予めＥＥＰＲＯＭ部１９に記憶されているＩＤデータを出力するように、ＩＣカード発行装置２のＭＰＵ１２が指示を出力する。

【００２３】この出力に基づいて、ＩＣカード３に内蔵されている制御部１８は、ＩＤデータをＥＥＰＲＯＭ部１９より読み出し、通信部１７を介してＩＣカード発行装置２に出力し、このＩＤデータが通信回線５を介してホストコンピュータ１に伝送される。

【００２４】このＩＤデータの出力により、ホストコンピュータ１は、記憶装置７内部に記憶されているデータベースから、このＩＤデータに対応付けられて記憶されている暗号鍵データ（ＫＡ）を検索するとともに、前記ランダムデータ生成装置９にて所定長のランダムデータ（ＴＲ）を生成し、このランダムデータ（ＴＲ）をＩＣカード発行装置２を介してＩＣカード３に出力する。

【００２５】次いでＩＣカード３では、このランダムデータ（ＴＲ）を前記暗号処理部２１にて、予めＥＥＰＲＯＭ部１９に記憶されている暗号鍵データ（ＫＢ）によって暗号化を実施し、この暗号化されたランダムデータ（ＡＲ）をＩＣカード発行装置２を介してホストコンピュータ１に返送する。

【００２６】ホストコンピュータ１では、この返送されてきた暗号化されたランダムデータ（ＡＲ）を、前記暗号生成装置８にて、前記検索された暗号鍵データ（ＫＡ）に基づき復元を実施して復元ランダムデータ（ＦＲ）とし、これら復元ランダムデータ（ＦＲ）と前記ランダムデータ（ＴＲ）とが一致するかを比較部において比較し、ＩＣカードが正規のものであるか否かの認証を実施し、その認証結果をＩＣカード発行装置２に出力する。

【００２７】この認証結果の出力に基づき、ＩＣカード発行装置２は、その認証結果が「否」である場合には、認証のエラーを前記ＬＣＤパネル１４に表示し、ＩＣカード３を排出して処理を終了し、その認証結果が「可」である場合には、ＬＣＤパネル１４に「発行スイッチを押して下さい」のメッセージを表示し、発行スイッチ５の入力待ちを所定時間行い、所定時間内に発行スイッチ５が入力されない場合には、ＩＣカード３を排出して、処理を終了する。

【００２８】発行スイッチ５が所定時間内に入力され場合には、ＩＣカード発行装置２は、ホストコンピュータ１に対して暗号化された復号鍵データ（ＰＡ）の出力を指示する。

【００２９】ホストコンピュータ１は、この指示により前記記憶装置７内部に記憶されている復号鍵データ（ＰＴ）を、前記検索された暗号鍵データ（ＫＡ）によって前記暗号生成装置８にて暗号化を実施し、暗号化された復号鍵データ（ＰＡ）を生成させ、これをＩＣカード発行装置２を介してＩＣカード３に出力する。

【００３０】この暗号化された復号鍵データ（ＰＡ）は、ＩＣカード３において、暗号化されたままの状態にて前記ＥＥＰＲＯＭ部１９に書き込み、記憶され、ＩＣカード３の制御部１８は、前記書き込みが終了すると書き込み完了をＩＣカード発行装置２に出力し、この出力に基づき、ＩＣカード発行装置２からＩＣカード３が排出されて、処理が終了する。

【００３１】このようにして前記ＥＥＰＲＯＭ部１９に記憶された暗号化された状態の復号鍵データ（ＰＡ）は、ＥＥＰＲＯＭ部１９に予め記憶されている暗号鍵データ（ＫＢ）により、必要に応じて前記暗号処理部２１にて復元されて使用されるようになっている。

【００３２】以上、本発明を図面基づいて説明してきたが、本発明は前記実施例に限定されるものではなく、本発明の主旨を逸脱しない範囲での変更や追加があっても、本発明に含まれることは言うまでもない。

【００３３】また、前記実施例では、ゲームプログラムのライセンスカードシステムを例として説明しているが、本発明はゲームプログラム以外のその他のプログラムデータ等においても同様の効果が得られることは言うまでもなく、それらプログラムデータが記憶される記憶媒体も、本実施例ではＣＤＲＯＭが使用されているが、これに限定されるものではなく、その他の記憶媒体であっても良い。

【００３４】また、本実施例では、前記ホストコンピュータ１に記憶されている暗号鍵データ（ＫＡ）とＩＣカード３に予め記憶されている暗号鍵データ（ＫＢ）とが、相関する１セットの組を形成しているものの、異なるデータとされているが、本発明はこれに限定されるも

のではなく、適宜な暗号化アルゴリズムを用いて、これら暗号鍵データを同一のものとするようにしても良い。

【００３５】また、本実施例では、復号鍵データを固定としているが、これら復号鍵データを、プログラムデータ毎に個別のものとしても良く、この場合においては、そのプログラムに対応する復号鍵データを特定するために、ホストコンピュータ１にＩＣカード発行装置２等からプログラムを特定可能とする情報、例えばプログラムナンバーや種別等を示す略号等を出力するようにして、そのプログラムだけを復号可能とするようにしても良い。

【００３６】また、前記ＩＣカード３をユーザー毎に個別のものとしておき、ＩＣカード３の前記ＥＥＰＲＯＭ部１９に、ユーザー情報等を記憶しておき、復号鍵データを書き込む際に、これらユーザー情報をホストコンピュータ１に出力させて、顧客管理が可能なようにしても良い。

【００３７】また、本実施例においては、前記ＩＣカード３の不揮発性メモリとしてＥＥＰＲＯＭを使用しているが、本発明はこれに限定されるものではなく、その他の不揮発性メモリ、例えば強誘電体メモリ（ＦｅＲＡＭ）やフラッシュメモリ等を使用しても良い。

【００３８】

【発明の効果】本発明は次の効果を奏する。

【００３９】（ａ）請求項１の発明によれば、ホストコンピュータより販売店およびＩＣカードに復号鍵データが配信、書き込まれる際に、ホストコンピュータより出力される復号鍵データが、ＩＣカードに個別に付与されたＩＤ等の識別データと関連付けられた暗号鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体が盗用されることなく、復号鍵データを販売店およびＩＣカードに配信、書き込むことができる。

【００４０】（ｂ）請求項２の発明によれば、ＩＣカード内部において、復号鍵データが暗号化された状態にて記憶されているため、第三者によって復号鍵データ自体をＩＣカード内部より読み出されて盗用されることを防ぐことができる。

【００４１】（ｃ）請求項３の発明によれば、仮にＩＣカードより暗号化された復号鍵データが盗用されたとしても、第三者によってＩＣカードより暗号鍵データが読み出されて、前記暗号化された復号鍵データが復元されることを防止できる。

【００４２】（ｄ）請求項４の発明によれば、書き込みがなされるＩＣカードが正規のＩＣカードであるか否かを暗号化された復号鍵データを出力する以前にホストコンピュータが確認できるばかりか、ホストコンピュータに識別データと関連付けて記憶されている復号鍵データに誤りが無いか否かを確認することもできる。

【００４３】

【図面の簡単な説明】

【図１】本発明の実施例における復号鍵データの書き込みシステムを用いたライセンスカードシステムを示す図である。

【図２】本発明の実施例における復号鍵データの書き込みシステムの各構成を示すブロック図である。

【図３】本発明の実施例におけるホストコンピュータに用いた暗号生成装置での処理内容を示す図である。

【図４】本発明の実施例におけるＩＣカードに用いた暗号処理部での処理内容を示す図である。

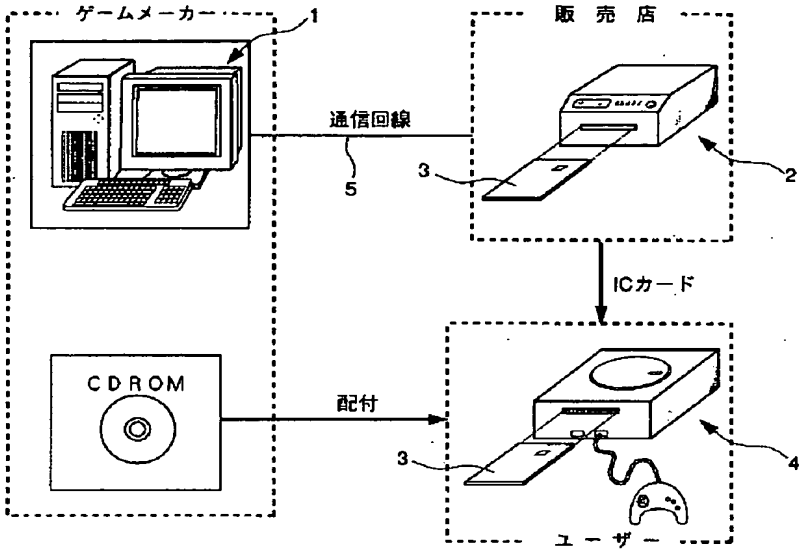
【図５】（ａ）、（ｂ）　本発明の実施例に用いたべき乗剰余演算アルゴリズムの処理概要を示す図である。

【図６】本発明の実施例におけるホストコンピュータとＩＣカード発行装置とＩＣカードとの処理動作を示す図である。

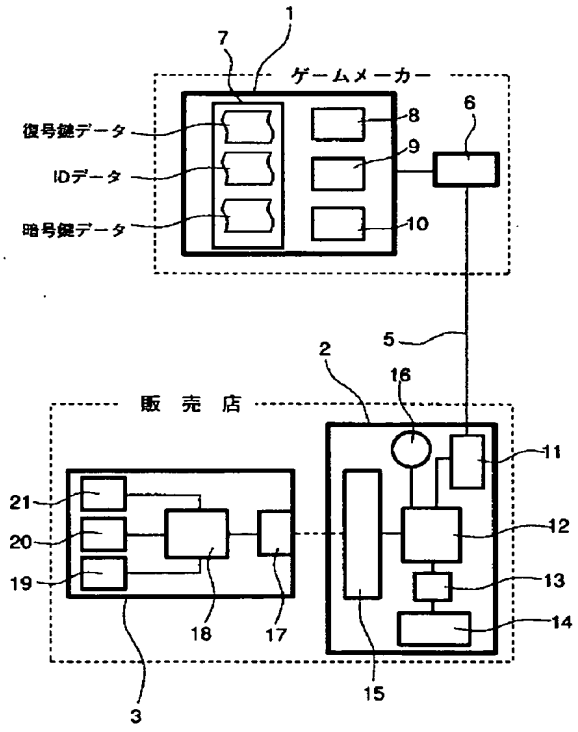
【符号の説明】

１	ホストコンピュータ
２	ＩＣカード発行装置
３	ＩＣカード
４	再生装置
５	通信回線（通信手段）
６	通信モデム（通信手段）
７	記憶装置
８	暗号生成装置
９	ランダムデータ生成装置
１０	比較部（比較手段）
１１	通信モデム部（通信手段）
１２	マイクロプロセッシングユニット（ＭＰＵ）
１３	ＬＣＤドライバ
１４	ＬＣＤパネル
１５	ＩＣカードリーダライタ部
１６	発行スイッチ
１７	通信部
１８	制御部
１９	ＥＥＰＲＯＭ部（不揮発性メモリ部）
２０	メモリ部
２１	暗号処理部

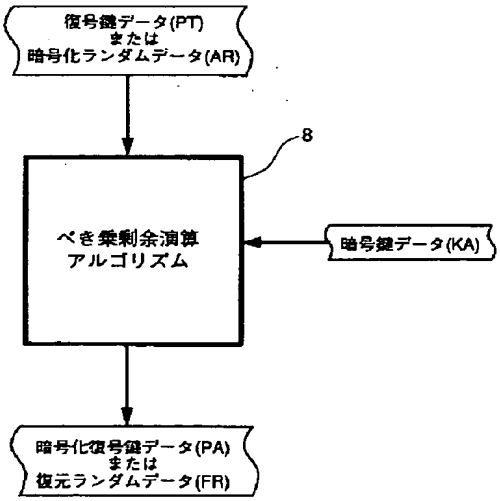
【図１】


ゲームメーカー
1
販売店
通信回線
5
3
2
ICカード
CDROM
配付
3
4
ユーザー

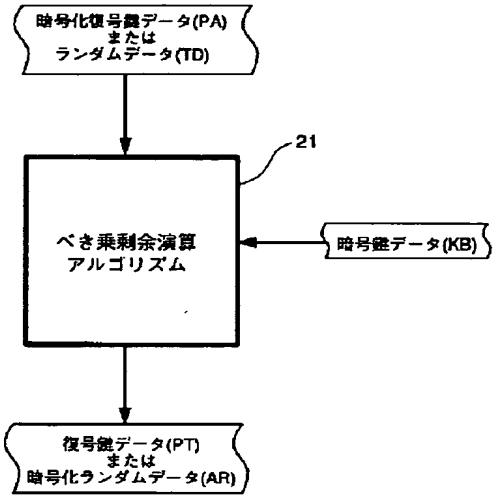
【図２】


1
7
ゲームメーカー
復号鍵データ
IDデータ
暗号鍵データ
8
9
10
6
5
2
16
販売店
11
12
13
14
21
20
19
18
17
3
15

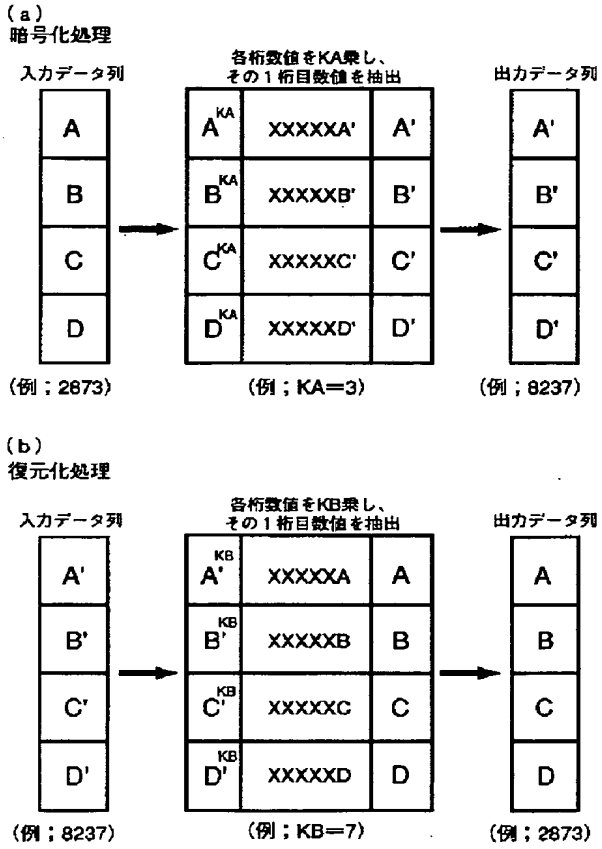
【図３】


復号鍵データ(PT)
または
暗号化ランダムデータ(AR)
8
べき乗剰余演算
アルゴリズム
暗号鍵データ(KA)
暗号化復号鍵データ(PA)
または
復元ランダムデータ(FR)

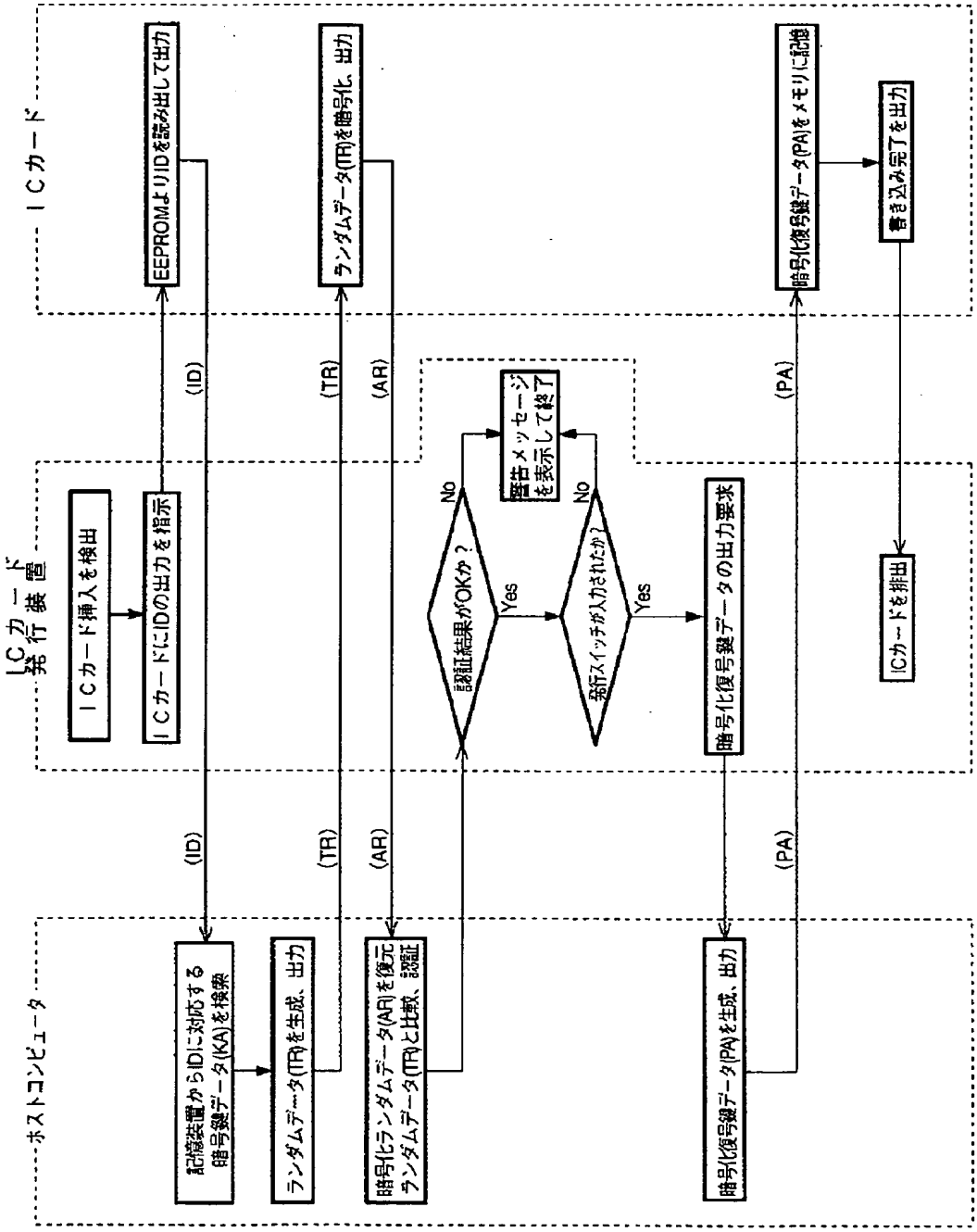
【図４】


暗号化復号鍵データ(PA)
または
ランダムデータ(TD)
21
べき乗剰余演算
アルゴリズム
暗号鍵データ(KB)
復号鍵データ(PT)
または
暗号化ランダムデータ(AR)

【図５】


(a)
暗号化処理
入力データ列
各桁数値をKA乗し、
その１桁目数値を抽出
出力データ列
A
B
C
D
A^KA
XXXXXA'
A'
B^KA
XXXXXB'
B'
C^KA
XXXXXC'
C'
D^KA
XXXXXD'
D'
A'
B'
C'
D'
(例；2873)
(例；KA=3)
(例；8237)
(b)
復元化処理
入力データ列
各桁数値をKB乗し、
その１桁目数値を抽出
出力データ列
A'
B'
C'
D'
A'^KB
XXXXXA
A
B'^KB
XXXXXB
B
C'^KB
XXXXXC
C
D'^KB
XXXXXD
D
A
B
C
D
(例；8237)
(例；KB=7)
(例；2873)

【図6】


ICカード
EEPROMよりIDを読み出して出力
ランダムデータ(TR)を暗号化 出力
暗号化復号鍵データ(PA)をメモリに記憶
書き込み完了を出力
(ID)
(TR)
(AR)
(PA)
IC力ード発行装置
ICカード挿入を検出
ICカードにIDの出力を指示
No
Yes
認証結果がOKか？
警告メッセージを表示して終了
No
発行スイッチが入力されたか？
Yes
暗号化復号鍵データの出力要求
ICカードを排出
(ID)
(TR)
(AR)
(PA)
ホストコンピュータ
記憶装置からIDに対応する暗号鍵データ(KA)を検索
ランダムデータ(TR)を生成、出力
暗号化ランダムデータ(AR)を復元ランダムデータ(TR)と比較、認証
暗号化復号鍵データ(PA)を生成、出力